Seguridad en Los Sistemas Distribuidos

PUA Mascheroni, Maximiliano Agustín

Introducción

- En la actualidad, las organizaciones son cada vez más dependientes de los sistemas distribuidos.
- La falta de medidas de seguridad en las redes es un problema que está en crecimiento.
- Los "incidentes de seguridad" crecen a la par de la masificación del Internet y de la complejidad del software desarrollado.
- La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo.

Políticas de seguridad

- En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles.
- Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de mecanismos de seguridad.
- Las políticas de seguridad informática surgen como una *herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento*.

- Las políticas de seguridad son planes de acciones o documentos que se utilizan como herramienta organizacional para afrontar riesgos de seguridad.
- La distinción entre ellas y los mecanismos de seguridad es de utilidad cuando se diseñan sistemas seguros, pero no es fácil estar seguro de que cierto conjunto de mecanismos de seguridad implementan completamente las políticas de seguridad deseadas.

Amenazas y Ataques

- En la mayoría de los tipos de redes locales es fácil construir un programa sobre un computador conectado para que obtenga copias de los mensajes transmitidos entre computadores.
- La principal meta de la seguridad es restringir el acceso a la información y los recursos de modo que sólo tengan acceso aquellos que estén autorizados.
- Las amenazas de seguridad se dividen en tres clases:

  • ***Fuga***: la adquisición de información por receptores no autorizados.

  • ***Alteración***: la modificación no autorizada de información.

  • ***Vandalismo***: interferencia en el modo de operación adecuado de un sistema, sin ganancia para el responsable.

- Los ataques en los sistemas distribuidos dependen de la obtención de acceso a los canales de comunicación.
- Los métodos de ataque pueden clasificarse en función del modo en que se abusa del canal:

  • ***Fisgar***: obtener copias sin autorización.

  • ***Suplantar****:* enviar o recibir mensajes utilizando la identidad de otro sin su autorización.

  • ***Alterar mensajes****:* interceptar mensajes y alterar sus contenidos antes de pasarlos al receptor.

  • ***Reenviar****:* almacenar mensajes interceptados y enviarlos más tarde.

  • ***Denegación de servicio****:* desbordar un canal o recurso para impedir que otros accedan a él.

  • ***Ataques desde código móvil****: Varios lenguajes de programación, han sido diseñados para permitir la descarga de programas desde servidores remotos y así lanzar procesos que se ejecutan localmente. En este caso, las interfaces internas y los objetos del interior de un proceso en ejecución pueden quedar expuestos a un ataque por código móvil.*

- Cuando se diseñó Internet y los sistemas conectados a ella, la seguridad no era una prioridad.
- Los diseñadores probablemente no tenían un concepto adecuado de la escala en que crecería Internet.
- La incorporación de medidas de seguridad requiere ser cuidadoso con la etapa de diseño.
- Los mecanismos de seguridad no pueden protegernos contra una clave de acceso mal elegida o custodiada

Seguridad de las Transacciones Electrónicas

- Muchas aplicaciones de Internet en la industria, el comercio y demás implican transacciones que dependen de la seguridad, como ser:
  - ***E-mail***
  - ***Compra de bienes y servicios***
  - ***Transacciones bancarias***
  - ***Micro-transacciones***

- Una política de seguridad sensata para vendedores y compradores de Internet exige los siguientes requisitos:

1) Autenticación del vendedor al comprador.
2) Mantenimiento del número de tarjeta de crédito y otros detalles del comprador bajo secreto, y asegurar que se transmiten de forma inalterada del comprador al vendedor.
3) Si los bienes se encuentran en una forma útil para su descarga, asegurar que su contenido llega al comprador sin alteración y sin ser desvelados a terceras partes.
4) Autenticar la identidad del titular de la cuenta hacia el banco antes de darle acceso a su cuenta.

Criptografía

- La criptografía proporciona la base para la mayoría de los sistemas de seguridad de los computadores.
- La encriptación es el proceso de codificación de un mensaje de forma que queden ocultos sus contenidos.
- La criptografía moderna incluye algunos algoritmos seguros de encriptación y desencriptación de mensajes. Todos ellos se basan en el uso de ciertos secretos llamados claves.
- Una clave criptográfica es un parámetro empleado en un algoritmo de encriptación de manera que no sea reversible sin el conocimiento de una clave.

- Hay dos clases principales de algoritmos de encriptación de uso general:
  - ***Con uso de claves secretas compartidas:*** donde el emisor y el receptor deben compartir el conocimiento de una clave y ésta no debe ser revelada a ningún otro.
  - ***Con uso de pares de claves pública/privada:*** donde el emisor de un mensaje emplea una clave pública, difundida previamente por el receptor para encriptar el mensaje, es decir, el receptor emplea la clave privada correspondiente para desencriptar el mensaje.

FINES DE LA CRIPTOGRAFÍA

- La criptografía juega tres papeles principales en la implementación de los sistemas seguros:
  - ***Secreto e integridad*: se emplea para mantener el secreto y la integridad de la información dondequiera que pueda estar expuesta a ataques potenciales.
  - ***Autenticación:*** La criptografía se emplea como base de los mecanismos para autenticar la comunicación entre pares de principales.
  - ***Firmas digitales*: Ésta emula el papel de las firmas convencionales, verificando a una tercera parte que un mensaje o un documento es una copia inalterada producida por el firmante.

ALGORITMOS CRIPTOGRÁFICOS:

- Un mensaje puede encriptarse mediante la aplicación de alguna regla que transforme el *texto claro* del mensaje a un *texto cifrado o criptograma* (esto lo realiza el emisor).
- El receptor debe conocer la regla inversa para transformar el texto cifrado en el texto original, mientras que el resto de los principales deben ser incapaces de descifrar el mensaje, a menos que conozcan esta regla inversa.
- La transformación de encriptación se define mediante dos elementos: una *función E* y una *clave K.* El mensaje resultante encriptado se escribe *{M}k.*

$$E(K,M) = \{M\}k$$

- La función de encriptación *E* define un algoritmo que transforma los datos de texto en datos encriptados al combinarlos con la clave y transformándolos de un modo que depende fuertemente del valor de la clave.
- La desencriptación se lleva a cabo empleando una función inversa D, que también toma como parámetro una clave:

$$D(K, E(K, M))=M$$

- Debido a este uso simétrico de las claves, a menudo se habla de la criptografía de clave secreta como *criptografía simétrica,* mientras que la criptografía de clave pública se denomina *asimétrica* debido a que las claves empleadas para el encriptado y el desencriptado son diferentes.

- **Algoritmos simétricos:** Si eliminamos de la consideración el parámetro de la clave y definimos Fk([M]) = *E(K, M),* una propiedad de las funciones de encriptación robustas es que Fk([M]) sea relativamente fácil de calcular, mientras que la inversa, Fk-1([M]) sea tan difícil de calcular que no sea factible.
- **Algoritmos asimétricos:** Cuando se emplea un par de claves pública / privada, las funciones de un solo sentido se explotan de otra forma. La base de todos los esquemas es la existencia de *funciones de puerta falsa.*
- **Cifradores de bloque.** La mayoría de los algoritmos de encriptación operan sobre bloques de datos de tamaño fijado: 64 bits es un tamaño de bloque popular. Cada mensaje se subdivide en bloques, el último bloque se rellena hasta la longitud estándar si fuera necesario y cada bloque se encripta independientemente. El primer bloque está listo para ser transmitido tan pronto como haya sido encriptado.

- **Diseño de algoritmos criptográficos:** Existen muchos algoritmos criptográficos bien diseñados tales que *E(K, M) = {M}k* oculta el valor de *M* y resulta prácticamente imposible recuperar *K* con mejor éxito que el que proporciona la fuerza bruta.
- Todos los algoritmos de encriptación se apoyan en manipulaciones que preservan la información de *M* y emplean principios basados en la teoría de la información que describe los principios de *confusión* y *difusión* para el ocultamiento del contenido del bloque de criptograma *M,* combinándolo con una clave *K* de tamaño suficiente para ponerlo a prueba de ataques por fuerza bruta.
- **Confusión:** Las operaciones de carácter no destructivo como XOR y el desplazamiento circular se emplean para combinar cada bloque de texto en claro con la clave, produciendo un nuevo patrón de bits que oscurece la relación entre los bloques de *M* y los de *{M}k.*
- **Difusión:** disipa la existencia de patrones regulares mediante la transposición de partes de cada bloque de texto en claro

ALGORITMOS DE CLAVE SECRETA (SIMÉTRICOS)

- TEA: se ha escogido por la simplicidad de su diseño e implementación.
- DES: ha sido un estándar nacional de los EE.UU., aunque su interés es histórico dado que sus claves de 56 bits son demasiado reducidas para resistir un ataque por fuerza bruta con el hardware actual.
- IDEA: emplea una clave de 128 bits y es, probablemente, el algoritmo de encriptación simétrico de bloques más efectivo y una elección muy acertada para el encriptado en masa.
- AES: también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

TEA

- Los principios de diseño para los algoritmos simétricos que se delinearon anteriormente se ven ilustrados en *Tiny Encryption Algorithm* (TEA, pequeño algoritmo de encriptación).
- Emplea vueltas de sumas enteras, XOR y desplazamientos lógicos de bits, para obtener la difusión y confusión de los patrones de bits en el texto en claro. El texto en claro es un bloque de 64 bits representado como dos enteros de 32 bits en el vector de texto [ ]. La clave tiene 128 bits representada como cuatro enteros de 32 bits.
- Esta clave es segura contra los ataques de fuerza bruta.
- En cada una de las 32 etapas, se combinan repetidamente las dos mitades del texto con porciones desplazadas de la clave y entre sí en las líneas 5 y 6 el empleo de XOR sobre porciones del texto desplazada introduce confusión y el desplazamiento e intercambio de las dos porciones del texto introduce difusión.
- La función de desencriptado es la inversa de función de encriptación.

DES

- El Estándar de Encriptación de Datos *(Data Encryption Standar)*, es el más usado para aplicaciones gubernamentales y de negocios.
- En este estándar la función de encriptación proyecta un texto en claro de 64 bits usando una clave de 56 bits.
- El algoritmo tiene 16 etapas dependientes de claves conocidas como *Vueltas* en las que el dato a encriptar se rota bit a bit un número de veces que depende de la clave y tres transposiciones no dependientes de la clave.
- A pesar de que aún se emplea en muchas aplicaciones comerciales y de otro tipo, DES, en su forma básica, debe considerarse obsoleta para la protección de aquello que no sea información de bajo interés.

IDEA

- El Algoritmo de Encriptación de Datos Internacional *(International Data Encription Algorithm,* IDEA) se desarrolló a comienzos de los años noventa como sucesor del DES.
- Como TEA, emplea una clave de 128 bits para encriptar bloques de 64 bits.
- El algoritmo se basa en el álgebra de grupos y tiene ocho vueltas XOR, suma módulo 216 y multiplicación. Tanto DES como IDEA emplean una misma función para la encriptación y desencriptación: una propiedad útil para los algoritmos que han de implementarse en hardware.
- La resistencia de IDEA ha sido analizada extensamente y no se han encontrado debilidades significativas, realiza la encriptación y desencriptación a una velocidad tres veces superior que la de DES.

AES

- En 1997, el Instituto Nacional para los Estándares y la Tecnología (NIST) publicó una invitación para remitir propuestas de un algoritmo seguro y eficiente que seria adoptado como nuevo Estándar de Encriptación Avanzada (Advanced Encryption Standard, AES)
- La comunidad de investigación sobre criptografía remitió quince algoritmos como respuesta a la invitación inicial para el AES. Tras una intensa inspección técnica se seleccionaron cinco de ellos para la siguiente fase de evaluación. Todos los candidatos soportaban claves de 128, 192 y 256 bits, siendo todos ellos de altas prestaciones. La evaluación concluyó en mayo del año 2000, cuando se seleccionó un estándar preliminar.

ALGORITMOS DE CLAVE PÚBLICA (ASIMÉTRICOS)

- Hasta la fecha sólo se han desarrollado unos pocos esquemas prácticos de clave pública y estos dependen del uso de funciones de puerta falsa de números grandes para producir las claves.
- **RSA:** (Rivest, Snamir y Adelman) es un algoritmo cuyo diseño para el encriptador de clave pública, se basa en el uso del producto de dos números primos muy grandes (mayores que 10^100).
- **Algoritmos de curvas elípticas:** Un algoritmo puede generar pares de claves pública/ privada basándose en las propiedades de las curvas elípticas. Las claves que derivan de una rama diferente de las matemáticas, y a diferencia de RSA su seguridad no dependen de la dificultad de la factorización de números grandes. En cambio las claves cortas son seguras, y los requisitos de procesamiento para la encriptación y la desencriptación son menores.

PROTOCOLOS CRIPTOGRÁFICOS HÍBRIDOS

- La criptografía de clave pública es apropiada para el comercio electrónico porque no hay necesidad de un mecanismo de distribución segura de claves.
- La criptografía de clave pública demanda costos elevados para la encriptación incluso de mensajes de tamaño medio como los que se encuentran habitualmente en el comercio electrónico.
- La solución adoptada en los sistemas distribuidos de gran escala es el empleo de un esquema de encriptación híbrido en el que se emplea criptografía de clave pública para autentificar cada parte y para encriptar un intercambio de claves secretas, que se emplearán para toda la comunicación subsiguiente.

FIRMAS DIGITALES

- Una firma digital robusta es un requisito esencial para los sistemas seguros. Se las necesita para certificar ciertos trozos de información, por ejemplo, para proporcionar enunciados dignos de confianza que relacionan identidades de usuarios con claves públicas.
- Las firmas manuscritas necesitan verificar que éste es:
  - ***Autentico***: convence al receptor de que el firmante firmó deliberadamente el documento y que la firma no ha sido alterado por nadie.
  - ***Infalsificable***: aporta la prueba de que el firmante firmó el documento.
  - ***No repudiable***: el firmante no puede negar de forma creíble que el documento fue firmado por él.

Certificados

- Un certificado digital es un documento que contiene una sentencia (generalmente corta) firmada por un principal.
- Se emplean para establecer la autenticidad de muchos tipos de enunciados.
- Para que los certificados sean útiles se requieren dos cosas:
  - Un formato estándar y una representación para ellos de modo que los emisores de certificados y los usuarios de certificados puedan construirlos e interpretarlos.
  - Un acuerdo sobre la forma en que se construyen las cadenas de certificados, y en particular la noción de autoridad fiable.
- El principal inconveniente es la dificultad al elegir una autoridad fiable de donde pueda arrancar una cadena de autenticaciones.
- La elección de una autoridad dependerá del objetivo para el que se necesite el certificado.

Credenciales

- Las credenciales son un conjunto de evidencias presentadas por un principal cuando pide acceso a un recurso.
- Las credenciales basadas en funciones parecen especialmente útiles en el diseño de esquemas de control de acceso prácticos.
- Los conjuntos de credenciales basadas en funciones se definen para las organizaciones o para tareas cooperativas, y los derechos de acceso de nivel de aplicación se construyen con referencia a ellas.

Delegación

- Una forma particularmente útil de credencial es aquella que permite a un principal, o proceso actuando para un principal, realizar una acción con la autoridad de otro principal (puede aparecer en cualquier situación donde un servicio necesite acceder a un recurso protegido para completar una acción en representación de su cliente).
- Se puede conseguir la delegación utilizando un certificado de delegación o una habilitación.
- El certificado está firmado por el principal solicitante y autoriza a otro principal para acceder a un recurso con nombre.
- La habilitación es un conjunto codificado e infalsificable de derechos de acceso al recurso logrando el mismo resultado sin necesidad de identificar a los principales.
- Cuando se delegan derechos, es común restringirse a un subconjunto de los derechos que posee el principal que lo emite, de este modo el principal delegado no podrá abusar de ellos.

Cortafuegos

- Es una parte del sistema o de la red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- Con ellos se protege una intranet, se realizan acciones de filtrado en las comunicaciones entrantes y salientes.
- El empleo de cortafuegos no ofrece protección contra los ataques desde el interior de una organización, y es ciertamente tosco en el control del acceso externo.
- En consecuencia existe una necesidad de mecanismos de seguridad de un grano más fino, que permitan a los usuarios individuales compartir información con otros usuarios seleccionados sin comprometer la privacidad y la integridad.
- Los cortafuegos no son particularmente útiles contra ataques de denegación de servicios, basado en la suplantación de direcciones IP.

Diseño de Sistemas Distribuidos Seguros

- El objetivo del diseñador es excluir todos los posibles ataques y agujeros.
- La situación es análoga a la del programador cuyo principal objetivo es excluir todos los errores de su programa.
- En ningún caso existe un método concreto para asegurar las metas durante el diseño.
- Cada uno diseña con los mejores estándares disponibles y aplica un análisis informal y comprobaciones
- Una vez que un diseño esté completo, una opción es la validación formal.
- Cuando se diseña para seguridad es necesario pensar siempre en lo peor.

Premisas del peor caso posible

- Las interfaces están desprotegidas
- Las redes son inseguras
- Límite en el tiempo de vida y el alcance de cada secreto
- Los algoritmos y el código de los programas están disponibles para los atacantes
- Los atacantes tienen acceso a suficientes recursos
- Minimícese la base de confianza

Recomendaciones de seguridad en sistemas distribuidos de cómputo

- Efectuar un análisis de riesgos
- Lo más valioso debe alejarse de lo más vulnerable
- Mantener las cosas simples
- Asegurar la seguridad en todos los niveles
- Encriptar tanto como sea posible
- No confiar en la autenticación estándar
- No usar la configuración "estándar“
- La seguridad hacia el interior
- Educar a los usuarios

- No confiar (totalmente) en nosotros mismos
- Ejecutar sólo los servicios imprescindibles
- Mantenerse al día con las actualizaciones
- Escaneos regulares
- Descargas de software de Internet
- Establecer planes de contingencia y sistemas de respaldo
- Mantener contacto con el proveedor de líneas de comunicación
- No permitir conexiones directas desde la red interna a Internet
- Uso de red perimétrica o zona desmilitarizada
- Prácticas de programación segura
- Vigilancia
- Establecimiento de políticas de seguridad

Sistemas de detección de intrusos

- Los Sistemas de detección de intrusos (IDS) son una de las tecnologías de más rápido crecimiento dentro del espacio de seguridad.
- ***Un sistema de detección de intrusos, es un programa usado para detectar accesos no autorizados a un computador o a una red.***
- Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.
- Se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.
- Desafortunadamente, muchas empresas tienen dificultades para ponerlos en uso debido a su complejidad de la implementación y la falta de información sobre su posible uso

Sistemas de prevención de intrusos

- Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
- La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.
- Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.

Conclusión

- La carencia del control de la seguridad de las redes es un tema que cada vez tiene una envergadura menor.
- El número de atacantes crece notablemente, y van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios
- La seguridad de la red requiere ir más allá de lograr que los sistemas simplemente funcionen bien. Se requiere creatividad (ser un cerrajero original), ciertas aptitudes de legislador (para proponer políticas adecuadas), así como un considerable conocimiento de la tecnología involucrada. Una dosis de paranoia puede ser indispensable.

Bibliografía

- George Coulouris. Sistemas Distribuidos. Addison Wesley. 3º Edición
- Coulouris Dolumore. Sistemas Distribuidos. Capítulo 7. Páginas (235 - 289). 3º Edición
- Roger S. Presuman. Ingeniería de Software. McGraw-Hill. 5º Edición
- A. S. Tanenbaum. Sistemas Operativos Distribuidos. Prentice Hall
- Rules definition for anomaly based intrusion detection. V1.1. Lubomir Nistor
- Intrusion Prevention Systems "Minimizando la ventana de riesgo". Alex Quintieri Fernández
- Securing the Broker Pattern. Patrick Morrison and Eduardo B. Fernandez.
- Dept. of Computer Science & Engineering, Florida Atlantic University.